(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 July 2001 (26.07.2001)

PCT

(10) International Publication Number
WO 01/53965 A1

(51) International Patent Classification⁷: G06F 15/173, 17/60, 17/27, 17/30

(21) International Application Number: PCT/AU00/00089

(22) International Filing Date: 10 February 2000 (10.02.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 5180 20 January 2000 (20.01.2000) AU

(71) Applicant (*for all designated States except US*): **ODYSSEY DEVELOPMENT PTY LTD** [AU/AU]; Suite 202, 10-12 Clarke Street, Crows Nest, NSW 2065 (AU).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): **DAVIES, Ian, Alexander** [AU/AU]; Suite 202, 10-12 Clarke Street, Crows Nest, NSW 2065 (AU).

(74) Agent: **F B RICE & CO.**; 605 Darling Street, Balmain, NSW 2041 (AU).

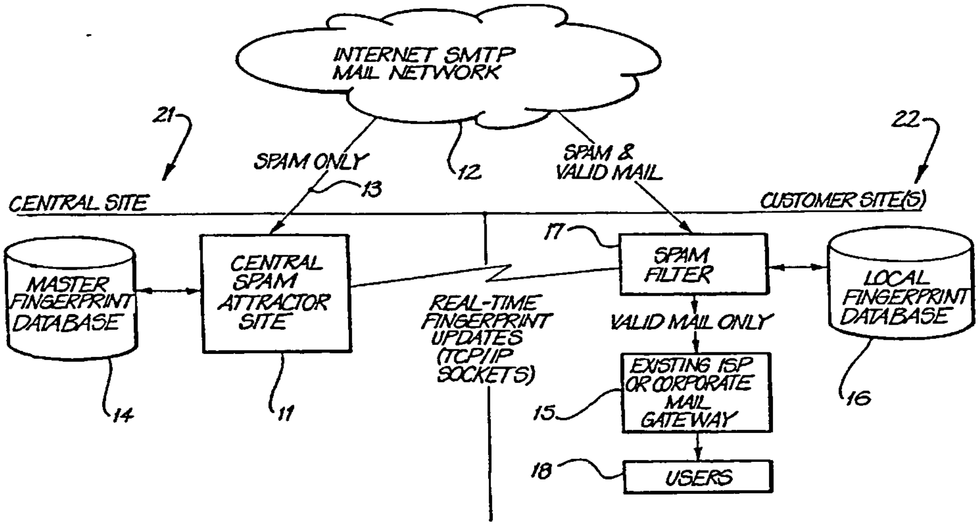
(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: E-MAIL SPAM FILTER


INTERNET SMTP MAIL NETWORK
21
22
SPAM ONLY
12
SPAM & VALID MAIL
13
CENTRAL SITE
CUSTOMER SITE(S)
17
MASTER FINGERPRINT DATABASE
CENTRAL SPAM ATTRACTOR SITE
SPAM FILTER
LOCAL FINGERPRINT DATABASE
REAL-TIME FINGERPRINT UPDATES (TCP/IP SOCKETS)
VALID MAIL ONLY
EXISTING ISP OR CORPORATE MAIL GATEWAY
14
11
16
15
18
USERS

(57) **Abstract:** Spam is attracted by creating a series of e-mail addresses held by a spam attractor site (11) connected to the internet SMTP mail network (12), that are used to engage in high risk activities known to attract spam. All spam received would be funnelled and subject to the same processing, regardless to which of the e-mail addresses it was actually sent to. All mails received at these e-mail addresses must be spam as the addresses are not provided to any other mail source. The mail is received, and the fingerprint is calculated for each message. The central fingerprint database (14) contains a relational table with the following structure, and one row for each unique item of spam detected. A spam filter is associated with each mail gateway and when an e-mail is received, the mail gateway calculates a mail signature using the fingerprint algorithm, the signature is looked up in the local database, and if found, the mail is discarded.

E-mail spam filter

Introduction

The present invention relates to the provision of e-mail services over the internet and in particular, it provides a method and system for filtering unsolicited material from an incoming stream.

Background of the Invention

Internet electronic mail (or, e-mail) is becoming increasingly clogged by unsolicited advertising material ("spam"), which causes network congestion and server overload for Internet Service Providers (ISPs) and corporations, as well as increased clutter for users.

Users dislike spam because it congests their in-tray, and imposes a "noise" level of rubbish they must sift through, looking for real e-mails.

ISPs and network managers dislike spam because it raises the volume of traffic their infrastructure must cope with, while not providing any real benefit to anyone. Thus their network infrastructure must be upgraded (at substantial expense) sooner than would otherwise be required.

Existing spam prevention schemes rely on identifying certain keywords and, if found, destroying the e-mail prior to delivery. Such schemes are error prone, and frequently delete "real" e-mails without notice simply because they happen to unwittingly contain certain words. The results of such incorrect detection may be drastic. For example, a customer sending you an e-mail about a "really sexy deal" may think you are not interested, whereas in fact you never received it because the spam filter found a word match. There can be very real and significant commercial consequences from such false matches.

Other schemes work by blocking e-mail from certain addresses or domains. Such systems are not very effective because spamers usually send from multiple addresses which exist only for a matter of hours. Effectively a "hit and run" technique.

Some internet domains and ISPs are infamous as being sources of spam, and some other ISPs and network managers have resorted to blocking all mail from those addresses. For example, it is relatively common for ISPs to completely block all mail from AOL, thus making it impossible to communicate with a bona fide person who is signed up through that ISP. Typically, spamers operate through very large ISPs, and so indiscriminate blocking from that ISP is guaranteed to also block a large number of bona fide people.

Thus the address blocking schemes, when applied to individual addresses are not effective against stopping spam (due to hit-and-run), and when applied to entire domains are far too destructive of authentic e-mails.

Summary of the Invention

Throughout this specification, the term "spam" will be used to designate "unsolicited e-mail", whether of an advertising nature or otherwise.

According to a first aspect, the present invention consists in a method of selecting and removing spam from a stream of mail, received by mail service or mail client, comprising the steps of:

i) establishing a decoy e-mail mailbox with a decoy e-mail address which is not used for communication with other parties;

ii) engaging in activities known to attract spam using the decoy mail address;

iii) monitoring the decoy mailbox for mail sent to the decoy address;

iv) generating a characteristic string for each e-mail received, which can be used to identify other differently addressed copies of the same e-mail;

v) creating a database of characteristic strings and adding new characteristic strings as they are generated;

vi) providing the database to a mail filter associated with the mail service or mail client;

vii) filtering a stream of mail received by the mail service or mail client to remove from the stream, any mail having a characteristic corresponding to a characteristic string contained in the database.

According to a second aspect, the present invention consists in a system for selecting and removing spam from a stream of mail received by a mail service or mail client comprising;

i) a decoy e-mail mailbox with a decoy e-mail address which is not used for communication with other parties;

ii) spam attracting means arranged to engage in activities known to attract spam, using the decoy e-mail address;

iii) monitoring means which monitors the decoy e-mail mailbox for mail sent to the decoy address;

iv) spam characteristic generating means arranged to generate a characteristic string for each e-mail received which can be used to identify other differently addressed copies of the same e-mail;

v) a database of characteristic strings to which each new characteristic string is added as it is generated.

vi) A mail filter associated with the mail service or mail client, the mail filter being arranged to monitor a stream of mail received by the mail service or mail client and to remove from the stream any mail having a characteristic matching one of the characteristic strings in the data base.

According to a third aspect, the present invention consists in a method of generating a database of spam characteristic strings for detecting spam in a stream of mail received by a mail service or mail client comprising the steps of:

i) establishing a decoy e-mail mailbox with a decoy e-mail address which is not used for communication with other parties;

ii) engaging in activities known to attract spam using the decoy e-mail address;

iii) monitoring the decoy mailbox for mail sent to the decoy address;

iv) generating a characteristic string for each e-mail received which can be used to identify other differently addressed copies of the same e-mail;

v) creating a database of characteristic strings and adding new characteristic strings as they are generated.

According to a fourth aspect, the present invention consists in a system for generating a database of spam characteristic strings used for detecting spam in a stream of mail received by a mail service or mail client comprising:

i) a decoy e-mail mailbox with a decoy e-mail address which is not used for communication with other parties;

ii) spam attracting means arranged to engage in activities known to attract spam, using the decoy e-mail address;

iii) monitoring means which monitors the decoy mailbox for mail sent to the decoy e-mail address;

iv) spam characteristic generating means arranged to generate a characteristic string for each e-mail received which can be used to identify other differently addressed copies of the same e-mail;

v) the database of characteristic strings being created by adding new characteristic string as it is generated.

According to a fifth aspect, the present invention consists in a method of selecting and removing spam from a stream of mail received by a mail service or mail client comprising the steps of:

i) creating a database of characteristic strings representing known spam messages received by a spam attractor;

ii) providing the database to a mail filter associated with the mail service or mail client.

iii) filtering a stream of mail received by the mail service or mail client to remove from the stream any mail having a characteristic which matches a characteristic string in the database.

According to a sixth aspect, the present invention consists in a system for selecting and removing spam from a stream of mail received by a mail service or mail client comprising:

i) a database of characteristic strings representing known spam messages received by a spam attractor; and

ii) a mail filter associated with the mail service or mail client, the mail filter being arranged to monitor a stream of mail received by the mail service or mail client and to remove from the stream any mail having a characteristic which matches a characteristic string in the database.

In large installations, the server carrying the decoy mailbox, the server monitoring the decoy mailbox and the filter should preferably be closely linked such that when a piece of spam is received by the decoy mailbox, its characteristic can be determined and added to the database used by the filter as quickly as possible. This will require high speed communications between the decoy mailbox, the monitoring server and the filter. In this context, the term high speed communications means any communications method which is faster than the store and forward method used in email delivery systems.

In smaller systems where imposing a delay in the mail stream would not impose massive storage requirements, it may be possible to have greater delays in the monitoring of the decoy mailbox and the passing of characteristics to the filter, by compensating for those delays with a delay in the mailstream. In a single user system, or small corporate delivery system, for example, the mail delivery system would check the decoy mailbox and generate any new characteristics for the filter before accessing any user mailboxes on the mail server. In such a system, it may not be necessary to even have a dedicated decoy mailbox as it may be possible to subscribe to a service to be provided with spam characteristics generated via a centralised spam attracting and database building system.

Large installations will make use of multiple decoy mailboxes to maximize detection and to allow characterisation of spam according to different attraction methods.

Embodiments of the invention make use of the following key concepts:

1. Actively attracting as much spam as possible to a central site.

2. Characterizing or "Fingerprinting" each item of spam based on its textual content.

3. At the ISPs and corporate mail gateways, refusing e-mails whose "fingerprint" matches that of a known piece of spam.

4. Providing a very rapid, real time link between the central spam attracting site and the mail gateways, so that new items of spam are immediately added to the remote sites characteristic database.

The "fingerprint" is constructed by a combination of linguistic, textual and numeric methods to yield a relatively short binary number that serves to identify the content of the spamed message, with a very high likelihood for uniqueness.

The scheme of the preferred embodiment has the following advantages over conventional spam suppression techniques:

1. Very low probability of a false match and the deletion of a message which is not actually spam.

2. Identifies spam regardless of the sender or sender's address, thus resistant to "hit-and-run" attacks.

3. Also has virus prevention applications. Simply forward a virus to the central spam attracting site, and automatic protection against that virus occurs for all subscribing clients.

The preferred scheme works by using a source of pure spam to leverage cleansing of mail streams that consist of a mixture of spam and non-spam. It is relatively easy to obtain a source of pure spam by creating one or more e-mail addresses that are made to engage in "high risk" activity known to attract spam. Because these e-mail addresses have no real interaction with real people, then any e-mail they receive must surely be spam.

Brief Description of the Drawings

Embodiments of the invention will now be described, by way of example with reference to the accompanying drawing figure which schematically illustrates the arrangement of components which form a system according to a preferred embodiment of the invention.

Detailed Description of the Preferred Embodiment

Attracting Spam

Spam is attracted by creating a series of e-mail addresses held by a spam attractor site 11 connected to the internet SMTP mail network 12, that are used to engage in high risk activities known to attract spam. This would include, but not be limited to:

1. Automatically posting a message to popular newsgroups every few weeks
2. Registering a HotMail account
3. Joining AOL
4. Creating public web pages with the e-mail address mentioned and linked via a mailto URL
5. Joining many mailing lists and notification lists, as many of these are on-sold to spamers.

It is expected that some ongoing manual activity will be required to ensure the spam attractor keeps attracting spam. For example, to ensure AOL and HotMail accounts stay active, ensure appropriate newsgroups are frequented, and periodically change e-mail addresses so that spamers do not realize they should prevent spam from being sent to one of the spam attractor e-mail addresses belonging to the spam attractor 11.

Such manual reviews would need to be conducted every few weeks, or more frequently depending on Internet environmental issues.

However, actual receipt or collection of spam mail 13 would be completely automated, and should occur as rapidly as possible.

While there can be no assumptions made as to the sequence in which spamers send mail, it would nevertheless be prudent to choose spam attractor e-mail addresses that occur low in the collating sequence, as the objective is to ensure the spam attractor receives the spam as soon as possible.

The spam attractor central site 11 is preferably connected to the Internet via a fast link, and as directly as possible, to minimize mail propagation delays.

The spam would be sent to the various e-mail addresses in use. All spam received would be funnelled and subject to the same processing, regardless to which of the e-mail addresses it was actually sent to.

However, e-mail addresses will be placed in different categories, depending on the type of spam attracting activities for which they were used.

For example, an e-mail address that was used to post a message to a newsgroup would receive the 'worst' kind of spam. However, another e-mail address that was used to join various mailing lists would be placed in a different category. As spam is received and added to the fingerprint database, note would be kept of which category e-mail address the spam was addressed. This allows subscribers to the service to nominate whether they want all mass e-mail to be blocked, or only spam but not subscribed mailing lists, etc.

Processing Performed by Spam Attractor

The spam attractor 11 located at a central site 21 must regularly and continuously make POP connections to the various mail servers at which it has e-mail addresses in use. This can be done using standard POP software components.

The mail is received, and the fingerprint is calculated for each message (described below). The central fingerprint database 14 contains a relational table with the following structure, and one row for each unique item of spam detected.

TABLE SPAMDATABASE

FINGERPRINT_CODE	VARCHAR	UNIQUE KEY
SOURCE_CATEGORY	CHAR(10)	
ACTUAL_MESSAGE_TEXT	LONG CHAR	
DATE_CREATED	DATE	
DATE_LAST_SEEN	DATE	

The following table maps the e-mail addresses receiving spam into the various categories. This table would be maintained as new e-mail addresses are created and maintained to ensure that spam is attracted from the best possible sources.

TABLE SOURCES

EMAIL_ADDRESS	VARCHAR	UNIQUE KEY
CATEGORY	CHAR(10)	

The following table is relatively static, containing one row per category, describing the attributes and details of the category. This table would only be maintained as new categories are created.

TABLE CATEGORIES

CATEGORY_CODE	CHAR(10)	UNIQUE KEY
CATEGORY_NAME	VARCHAR	

The processing logic is as follows:

1. Obtain message.
2. Calculate fingerprint code.
3. Indexed lookup into Fingerprints table.
4. If found, confirm the category and update LastSeen date.
5. If not found, add to table. Set category based on e-mail address receiving message after looking up in Sources table. Store copy of message for reference purposes in Actual_Message_Text field. Set Created date.
6. If record was added to table, activate Notification Processor logic, as described below.

Periodically, records which have not been seen for more than some period of time (for example, 30 days) will be purged from the table to ensure performance and limit data volumes.

Fingerprint Algorithm

There are many possible methods of calculating the fingerprint code, and in practice the method may be varied over time to combat countermeasures spamers may employ.

The core method is to first dispose of the SMTP envelope which contains information about the e-mail and the path it took.

From there, compute a binary signature over the remainder of the body of the message. There are a variety of algorithms that can be used to compute a signature, for example, a simple CRC or HMAC (Key-hashing for Message Authentication) algorithm.

A better implementation could use a standard n-gram resemblance/containment algorithm or other similarity algorithm. Many such algorithms exists, and most have the desirable characteristics of some degree of fuzziness, and relatively small signature code lengths. Fuzziness is desirable as it means that e-mails that are substantially the same, except for minor variation, will be considered to match.

Outgoing notification processor

As new items of spam are detected by the above logic, it is essential that this fact is passed on to customer gateways 15 of the various customer sites 22 as soon as possible. Sending such notification via e-mail is not satisfactory, as it is very likely the notification will arrive substantially after the spam stream it is attempting to block. Instead, this should be done by sending TCP/IP packets directly from server to customer. This is done by the Notification Processor.

The Notification Processor is advised as new spam is identified. New spam is placed in a queue, containing the spam signature and the category.

The Notification Processor contains database information identifying all the customers who have subscribed to the service, and which categories they wish to be informed of. This could be implemented using the following tables:

TABLE CUSTOMERS

CUSTOMER_ID	NUMERIC
IP_ADDRESS	VARCHAR
PORT_NUMBER	NUMERIC
PRIORITY_CLASS	NUMERIC

TABLE CUSTOMER_CATEGORIES

CUSTOMER_ID	VARCHAR
CATEGORY_CODE	CHAR(10)

When a new spam item is placed in the outgoing queue, the Notification Processor performs a SELECT on these two tables to determine which customers wish to obtain notifications for spam of that category, what the customers IP address is, and with what priority the customer is to be processed. These are queued in priority sequence. Priority of individual customers may be set according to commercial or other consideration.

The Notification Processor continually works its queue, sending notifications. Each notification is a small TCP/IP packet sent to the customers chosen IP address and port number, containing the spam signature and category code.

The Notification Processor opens multiple TCP/IP sockets at a time, so that individual slow customers do not impact other customers further down the queue. The maximum number of concurrent sockets is a tuning parameter, but would be started at some value such as 10. Failed transmissions are added to the end of the queue for customers of the same priority level. If the same notification to that customer fails again, it is added to the end of the queue for customers of the next lowest (less important) priority. Failed notifications that reach the lowest level of priority and still fail are logged and discarded.

Note that due to timing considerations, it is possible that some spam items may arrive at the customer site before the notification packet arrives. However, since mail operates on a store and forward basis, whereas notification goes through TCP/IP directly, it is anticipated this will be minimal.

Mail gateway integration

Software is installed at the customer site which integrates at a SendMail level with the customers existing mail gateway 15. Where the customer runs multiple mail servers, integration would occur with each mail gateway separately, rather than centrally and then dispersed to the individual mail gateways. This gives better performance and distributes load.

The processing that occurs in the spam filter 17 associated with the mail gateway 15 is as follows. When each e-mail is received, the mail gateway calculates a mail signature using the same algorithm as the central site. The signature is looked up in the local database 16, and (subject to user-level over-ride processing described below), if found is discarded. If not found the e-mail is allowed to pass through.

For e-mails that are deleted, statistics are kept so that administrators can see the effectiveness of the system.

Additionally, the mail gateway listens on the specified IP address and port number to receive notifications from the central site of new spam items. Such entries are simply added to the local database 16.

Periodically, the local database is scanned and old entries are expired for space management reasons. This could be done daily or weekly.

User-level over-rides

Although a site may opt to receive notifications for various levels of spam, it is desirable to allow individual users 18 the option of not having spam blocked in that category.

For example, a site may opt for maximum protection and prevent spam from all categories. However, a bona fide user may wish to join a particular mailing list.

For this reason, the filter 17 associated with the customer mail gateway 15 must also contain a table of user over-rides, as follows

TABLE USER_OVERRIDES

USER_ADDRESS	VARCHAR
SENDER_ALLOWED	VARCHAR

The table is used as follows. When a matching spam message is detected, the mail gateway filter 17 inspects who the spam was being sent to, and what address it was being sent from. It does a lookup using these compound keys and, if found, allows the e-mail to proceed.

Most bona fide mail list servers and other sources of mail that may be mistaken for spam tend to be sent from fixed e-mail addresses, and so the sender address should be a reliable method of identification.

Further application: Viruses.

This process can also be applied to the prevention of propagation of e-mail computer viruses. Once a virus has come to the attention of a human operator, the virus is simply forwarded to the central spam attractor, and all client sites will thereafter be automatically protected against receipt of the virus.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A method of selecting and removing spam from a stream of mail, received by mail service or mail client, comprising the steps of:

i) establishing a decoy e-mail mailbox with a decoy e-mail address which is not used for communication with other parties, other than in spam attracting activities;

ii) engaging in activities known to attract spam using the decoy mail address;

iii) monitoring the decoy mailbox for mail sent to the decoy address;

iv) generating a characteristic string for each e-mail received, which can be used to identify other differently addressed copies of the same e-mail;

v) creating a database of characteristic strings and adding new characteristic strings as they are generated;

vi) providing the database to a mail filter associated with the mail service or mail client;

vii) filtering a stream of mail received by the mail service or mail client to remove from the stream, any mail having a characteristic corresponding to a characteristic string contained in the database.

2. The method of claim 1, wherein the decoy mailbox, the step of monitoring the decoy mailbox and the filtering step are implemented on a common server.

3. The method of claim 2, wherein delays in the monitoring of the decoy mailbox and the passing of characteristic strings to the filtering step, are compensated for by a delay in the stream of mail to be filtered by the filtering step.

4. The method of claim 1, wherein the decoy mailbox is implemented on a first server and the filtering step is implemented on a second server.

5. The method of claim 4, wherein high speed communication is provided between the first and second servers, such that when a piece of spam is received by the decoy mailbox the characteristic string of the spam is determined and quickly added to the database used by the filtering step.

6. The method of claim 5, wherein the step of monitoring the decoy mailbox is implemented on the first server.

7. The method of claim 4, wherein delays in the monitoring of the decoy mailbox and the passing of characteristic string to the filtering step, are

compensated for by a delay in the stream of mail to be filtered by the filtering step.

8. The method of claim 7, wherein the step of monitoring the decoy mailbox is implemented on the second server.

9. The method of claim 8, wherein the mail delivery system examines the decoy mailbox and generates any new characteristic strings for the filter before accessing any user mailboxes on the mail server.

10. The method of claim 7, wherein spam characteristic string are generated by a remotely located centralized spam attracting and database building system, and the database is updated from the centralized database building system for use in the filtering step.

11. The method of claim 1, wherein multiple decoy mailboxes are provided and different attraction methods are used with different decoy mailboxes and spam is characterized according to the attraction methods used.

12. The method of claim 1, wherein the step of generating a characteristic string makes use of linguistic, textual and/or numeric encoding methods.

13. The method of claim 12, wherein the step of generating a characteristic string comprises generating a Cyclic Redundancy Code on the content of the email.

14. The method of claim 12, wherein the step of generating a characteristic string comprises performing a Key-Hashing for Message Authentication (HMAC) on the content of the email.

15. The method of claim 1, wherein the step of generating a characteristic string disregards information relating to a sender or sender's address.

16. A system for selecting and removing spam from a stream of mail received by a mail service or mail client comprising;

i) a decoy e-mail mailbox with a decoy e-mail address which is not used for communication with other parties, other than in spam attracting activities;

ii) spam attracting means arranged to engage in activities known to attract spam, using the decoy e-mail address;

iii) monitoring means which monitors the decoy e-mail mailbox for mail sent to the decoy address;

iv) spam characteristic generating means arranged to generate a characteristic string for each e-mail received which can be used to identify other differently addressed copies of the same e-mail;

v) a database of characteristic strings to which each new characteristic string is added as it is generated;

vi) a mail filter associated with the mail service or mail client, the mail filter being arranged to monitor a stream of mail received by the mail service or mail client and to remove from the stream any mail having a characteristic matching one of the characteristic strings in the data base.

17. The system of claim 16, wherein the decoy mailbox, and the decoy mailbox monitoring means and the filter are implemented on a common server.

18. The system of claim 17, wherein delay means are provided to delay the stream of mail to the filter to compensate for delays in the monitoring of the decoy mailbox and the passing of characteristic strings to the filter.

19. The system of claim 16, wherein the decoy mailbox, is implemented on a first server and the filter is implemented on a second server.

20. The system of claim 19, wherein the first and second servers are linked by a high speed communications means, such that when a piece of spam is received by the decoy mailbox the characteristic string of the spam is determined and quickly added to the database used by the filter.

21. The system of claim 20, wherein the monitoring means for monitoring the decoy mailbox is implemented on the first server.

22. The system of claim 20, wherein delay means are provided to delay the stream of mail to the mail client to compensate for delays in the monitoring of the decoy mailbox and the passing of characteristic strings to the filter.

23. The system of claim 22, wherein the monitoring means for monitoring the decoy mailbox is implemented on the second server.

24. The system of claim 23, wherein the monitoring means examines the decoy mailbox and generates characteristic strings of newly received spam for the filter before the mail delivery system accesses any user mailboxes on the mail server.

25. The system of claim 22, wherein a remotely located centralized spam attracting and database building system is provided to attract spam and generate spam characteristic strings, and a local database of characteristic

strings is updated from the centralized database building system for use in the filtering step.

26. The system of claim 16, wherein multiple decoy mailboxes are provided and the spam attracting means operates a plurality of attraction methods which it associates with different decoy mailboxes and characterizes spam according to the attraction methods used.

27. The system of claim 16, wherein the characteristic string generating means makes use of linguistic, textual and/or numeric encoding methods.

28. The system of claim 27, wherein the characteristic string generating means makes use of a Cyclic Redundancy Code (CRC) algorithm.

29. The system of claim 27, wherein the characteristic string generating means makes use of a Key-Hashing for Message Authentication (HMAC) algorithm.

30. The system of claim 16, wherein the characteristic string generating means uses an algorithm which disregards a sender or sender's address of the email.

31. A method of generating a database of spam characteristic strings for detecting spam in a stream of mail received by a mail service or mail client comprising the steps of

i) establishing a decoy e-mail mailbox with a decoy e-mail address which is not used for communication with other parties, other than in spam attracting activities;

ii) engaging in activities known to attract spam using the decoy e-mail address;

iii) monitoring the decoy mailbox for mail sent to the decoy address;

iv) generating a characteristic string for each e-mail received which can be used to identify other differently addressed copies of the same e-mail;

v) creating a database of characteristic strings and adding new characteristic strings as they are generated.

32. The method of claim 1, wherein the decoy mailbox, and the step of monitoring the decoy mailbox are implemented on a common server.

33. The method of claim 32, wherein delays in the monitoring of the decoy mailbox and the adding of characteristic strings to the database of characteristic strings, are compensated for by a delay in the stream of mail to the mail client.

34. The method of claim 31, wherein the decoy mailbox is implemented on a first server, and the step of monitoring the decoy mailbox and building a database of spam characteristic strings is implemented on a second server.

35. The method of claim 34, wherein, high speed communication is provided between the first and second servers, such that when a piece of spam is received by the decoy mailbox the characteristic string of the spam is determined and quickly added to the database.

36. The method of claim 34, wherein delays in the monitoring of the decoy mailbox and the adding of characteristic string to the database of characteristic strings, are compensated for by a delay in the stream of mail to the mail client.

37. The method of claim 36, wherein the mail delivery system examines the decoy mailbox and generates any new characteristic strings for the database before accessing any user mailboxes on the mail server.

38. The method of claim 31, wherein the decoy mailbox, and the decoy mailbox monitoring function are implemented in a remotely located centralized spam attracting and database building system which generates spam characteristic strings, and a local database is updated from the centralized database building system for use when accessing the mail service.

39. The method of claim 31, wherein multiple decoy mailboxes are provided and different attraction methods are used with different decoy mailboxes and spam is characterized according to the attraction methods used.

40. The method of claim 31, wherein the step of generating a characteristic string makes use of linguistic, textual and/or numeric encoding methods.

41. The method of claim 40, wherein the step of generating a characteristic string comprises generating a Cyclic Redundancy Code on the content of the email.

42. The method of claim 40, wherein the step of generating a characteristic string comprises performing a Key-Hashing for Message Authentication (HMAC) on the content of the email.

43. The method of claim 31, wherein the step of generating a characteristic string disregards information relating to a sender or sender's address.

44. A system for generating a database of spam characteristic strings used for detecting spam in a stream of mail received by a mail service or mail client comprising:

i) a decoy e-mail mailbox with a decoy e-mail address which is not used for communication with other parties, other than in spam attracting activities;

ii) spam attracting means arranged to engage in activities known to attract spam, using the decoy e-mail address;

iii) monitoring means which monitors the decoy mailbox for mail sent to the decoy e-mail address;

iv) spam characteristic generating means arranged to generate a characteristic string for each e-mail received which can be used to identify other differently addressed copies of the same e-mail;

v) the database of characteristic strings being created by adding new characteristic string as it is generated.

45. The system of claim 44, wherein the decoy mailbox, and the decoy mailbox monitoring function are implemented on a common server.

46. The system of claim 45, wherein delay means are provided to delay the stream of mail to the mail client to compensate for delays in the monitoring of the decoy mailbox and the passing of characteristic strings to the database.

47. The system of claim 44, wherein the decoy mailbox, is implemented on a first server and the monitoring means for monitoring the decoy mailbox is implemented on a second server.

48. The system of claim 47, wherein the first and second servers are linked by a high speed communications means, such that when a piece of spam is received by the decoy mailbox the characteristic string of the spam is determined and quickly added to the database.

49. The system of claim 47, wherein delay means are provided to delay the stream of mail to the mail client to compensate for delays in the monitoring of the decoy mailbox and the adding of characteristic strings to the database.

50. The system of claim 47, wherein the database of spam characteristic strings are implemented on the second server.

51. The system of claim 50, wherein delay means are provided to delay the stream of mail to the mail client to compensate for delays in the monitoring of the decoy mailbox and the adding of characteristic string to the database.

52. The system of claim 51, wherein the monitoring means examines the decoy mailbox and generates characteristic strings of newly received spam for the database before the mail delivery system accesses any user mailboxes on the mail server.

53. The system of claim 44, wherein a remotely located centralized spam attracting and database building system is provided to attract spam and generate spam characteristic strings, and a local database of characteristics is updated from the centralized database building system for use when the mail delivery system accesses the mail service.

54. The system of claim 44, wherein multiple decoy mailboxes are provided and the spam attracting means operates a plurality of attraction methods which it associates with different decoy mailboxes and characterizes spam according to the attraction methods used.

55. The system of claim 44,, wherein the characteristic string generating means makes use of linguistic, textual and/or numeric encoding methods.

56. The system of claim 55, wherein the characteristic string generating means makes use of a Cyclic Redundancy Code (CRC) algorithm.

57. The system of claim 55, wherein the characteristic string generating means makes use of a Key-Hashing for Message Authentication (HMAC) algorithm.

58. The system of claim 44, wherein the characteristic string generating means uses an algorithm which disregards a sender or sender's address of the email.

59. A method of selecting and removing spam from a stream of mail received by a mail service or mail client comprising the steps of:

i) creating a database of characteristic strings representing known spam messages received by a spam attractor;

ii) providing the database to a mail filter associated with the mail service or mail client.

iii) Filtering a stream of mail received by the mail service or mail client to remove from the stream any mail having a characteristic which matches a characteristic string in the database.

60. The method of claim 59, wherein the step of creating the database and the filtering step are implemented on a common server.

61. The method of claim 60, wherein delays in the step of creating the database is compensated for by a delay in the stream of mail to the filter.

62. The method of claim 59 wherein the step of creating the database is implemented on a first server and the filtering step is implemented on a second server.

63. The method of claim 62, wherein high speed communication is provided between the first and second servers, such that when a piece of spam is added to the database of characteristic strings it is quickly made available to the filtering step.

64. The method of claim 62, wherein delays in creation of the database and the passing of characteristic strings to the filtering step, are compensated for by a delay in the stream of mail to be filtered by the filtering step.

65. The method of claim 64,wherein the mail delivery system updates the database of characteristic strings before accessing any user mailboxes on the mail server.

66. The method of claim 64, wherein spam characteristic strings are generated by a remotely located centralized spam attracting and database building system, and a local database is updated from the centralized database building system for use by the filtering step .

67. The method of claim 59, wherein an algorithm for generating the characteristic strings makes use of linguistic, textual and/or numeric encoding methods.

68. The method of claim 67, wherein an algorithm for generating the characteristic strings makes use of a Cyclic Redundancy Code (CRC) algorithm.

69. The method of claim 67, wherein the characteristic string generating means makes use of a Key-Hashing for Message Authentication (HMAC) algorithm.

70. The method of claim 59, wherein the characteristic string generating means uses an algorithm which disregards a sender or sender's address of the email.

71. A system for selecting and removing spam from a stream of mail received by a mail service or mail client comprising:

i) a database of characteristic strings representing known spam messages received by a spam attractor; and

ii) a mail filter associated with the mail service or mail client, the mail filter being arranged to monitor a stream of mail received by the mail service or mail client and to remove from the stream any mail having a characteristic which matches a characteristic string in the database.

72. The system of claim 71, wherein the database of characteristic strings and the filter are implemented on a common server.

73. The system of claim 72, wherein delay means are provided to delay the stream of mail to the mail client to compensate for delays in updating the database of characteristic strings and the passing of characteristic strings to the filter.

74. The system of claim 71,wherein the database of characteristic strings is implemented on a first server and the filter is implemented on a second server.

75. The system of claim 74, wherein the first and second servers are linked by a high speed communications means, such that when a characteristic string of a piece of spam is added to the database it is quickly passed to the filter.

76. The system of claim 75, wherein delay means are provided to delay the stream of mail to the filter to compensate for delays in the adding of characteristic strings to the database and the passing of characteristic strings to the filter.

77. The system of claim 71, wherein the database of characteristic strings is updated with characteristic strings of new spam before the mail delivery system accesses any user mailboxes on the mail server.

78. The system of claim 76, wherein a remotely located centralized spam attracting and database building system is provided to attract spam and generate spam characteristic strings, and a local database of characteristics is updated from the centralized database building system for use by the filter.

79. The system of claim 71, wherein an algorithm for generating the characteristic strings makes use of linguistic, textual and/or numeric encoding methods.

80. The system of claim 79, wherein an algorithm for generating the characteristic strings makes use of a Cyclic Redundancy Code (CRC) algorithm.

81. The system of claim 79, wherein the characteristic string generating means makes use of a Key-Hashing for Message Authentication (HMAC) algorithm.

82. The system of claim 71, wherein the characteristic string generating means uses an algorithm which disregards a sender or sender's address of the email.

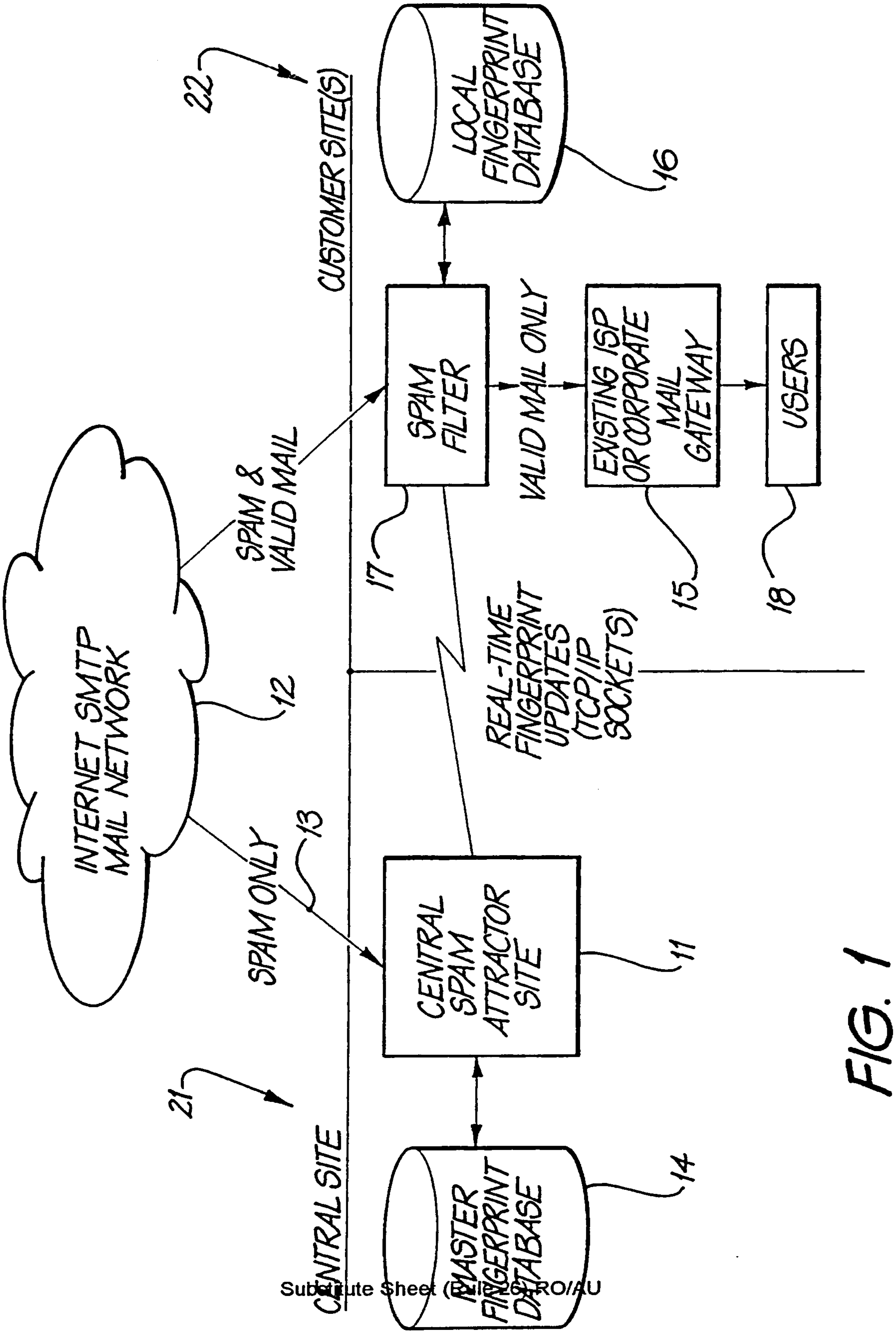

INTERNET SMTP MAIL NETWORK
12
SPAM & VALID MAIL
SPAM ONLY
13
CENTRAL SITE
21
CUSTOMER SITE(S)
22
CENTRAL SPAM ATTRACTOR SITE
11
MASTER FINGERPRINT DATABASE
14
SPAM FILTER
17
LOCAL FINGERPRINT DATABASE
16
VALID MAIL ONLY
EXISTING ISP OR CORPORATE MAIL GATEWAY
15
USERS
18
REAL-TIME FINGERPRINT UPDATES (TCP/IP SOCKETS)

FIG. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU00/00089

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. ^{7}: G06F 15/173, 17/60, 17/27, 17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT, INSC Keywords

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO9933188 (BRIGHT LIGHT TECHNOLOGYIES INC) 1 July 1999 - see whole document	1-82
A	GB2317793 (SECURE COMPUTING CORPORATION) 1 April 1998 - see whole document	
A	US5530853 (SCHELL et al) 25 June 1996 - see whole document	

□ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 13 March 2000	Date of mailing of the international search report 20 MAR 2000
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer Stephen Lee Telephone No : (02) 6283 2205

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU00/00089

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member	
WO	9933188	AU	16311/99
GB	2317793	DE	19741238
US	5530853	JP	6202918
			END OF ANNEX